IN THE SPECIFICATION:

Replace the section of the specification entitled "BRIEF DESCRIPTION OF THE DRAWINGS" with the following new section:

FIGURE 1 shows an example of an encryption process with a common secret key in a smart card;

FIGURE 2 shows a key XOR used in typical common key encryption;

FIGURE 3 shows a linear transform used in typical common key encryption;

FIGURE 4 shows a nonlinear transform used in typical common key encryption;

FIGURE 5 shows an example of encryption performed by a combination of the key XOR (FIGURE 2) and the nonlinear transform (FIGURE 4) in series connection;

FIGURE 6 shows elements related to an arbitrary nonlinear transform element wi shown in FIGURE 5;

FIGURES 7A and 7B show dissipated power curves representative of change of the electric dissipated power with time in an encryption processor in response to input plaintext into the processor;

FIGURE 7C shows difference between the dissipated power curves, which has a spike;

FIGURE 7D shows difference between the dissipated power curves, which has no spike;

FIGURE 8 shows an encryption device having a configuration in which two linear transforms are added before and after the encryption device of FIGURE 4;

FIGURE 9 shows measured points A, B and C for measuring dissipated power curves in the encryption device of FIGURE 5;

FIGURE 10 shows a schematic block diagram of the process in accordance with the random mask value method;

FIGURE 11 shows a key XOR in accordance with the random mask value method;

FIGURE 12 shows a linear function in accordance with the random mask value method;

FIGURES 13A and 13B shows a nonlinear function in accordance with the random mask value method;

FIGURE 14 shows a general configuration of a conventional N-round Rijndael process without protection against the DPA;

FIGURE 15 shows a sub-key generator for generating sub-keys, K0, K1, ... KN, from a secret key Ksec in the Rijndael method;

FIGURE 16 shows a configuration of the Subbyte;

FIGURE 17 shows a configuration of the Shift;

FIGURE 18 shows a configuration of the Mixedcolumn;

FIGURE 19 shows the N-round Rijndael method employing the random mask value method as opposed to the conventional N-round Rijndael method shown in FIGURE 14;

FIGURE 20 shows a configuration of a NewSBox used for providing sixteen SBoxes in the process of FIGURE 19;

FIGURE 21 shows a schematic configuration of a first type of encryption device in accordance with the invention;

FIGURE 22 shows a configuration of a key XOR used in the device of FIGURE 21;

FIGURE 23 shows a configuration of a nonlinear transform used in the device of FIGURE 21;

FIGURE 24 shows a schematic configuration of a second type of encryption device in accordance with the invention;

FIGURE 25 shows a configuration of a key XOR used in the device in FIGURE 24;

FIGURE 26 shows a configuration of a nonlinear transform used in the device in FIGURE 24;

FIGURE 27 shows an example of the first type of encryption device of FIGURE 21;

FIGURE 28 shows a configuration of the Subbyte shown in FIGURE 27;

FIGURE 29 shows another example of the first type of encryption device of FIGURE 21;

FIGURE 30 shows a configuration of the Subbyte shown in FIGURE 29;

FIGURE 31 shows an example of the second type of encryption device of FIGURE 24;

FIGURES 32A and 32B shows a configuration of a conventional DES;

FIGURES 33A and 33B shows a configuration of the Feistel DES employing the fixed mask value method shown in FIGURE 29;

FIGURES 34A and 34B shows a configuration of the Feistel DES employing the fixed mask value method shown in FIGURE 31;

FIGURE 35 shows propagation of the mask over the rounds in the encryption in the Feistel encryption device; and

FIGURE 36 shows paths from the generation of a mask to cancellation of the mask value in the Feistel encryption device.